World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Security challenges in civil registration: safeguarding vital information in an evolving landscape

Peter Kennedy Okoth *

Jaramogi Oginga Odinga University of Science & Technology, Kenya.

World Journal of Advanced Research and Reviews, 2023, 19(01), 1051–1071

Publication history: Received on 04 June 2023; revised on 19 July 2023; accepted on 21 July 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.19.1.1203

Abstract

Civil registration is a fundamental process that captures vital events such as births, deaths, marriages, and divorces, enabling governments to create accurate demographic databases and deliver essential services to their citizens. However, in today's digital age, civil registration systems face numerous security challenges that jeopardize the integrity and confidentiality of vital information. This paper highlights some of the key security challenges encountered in civil registration systems and outlines potential strategies to address them. Firstly, the digitization of civil registration processes has opened new avenues for cyber threats. Malicious actors may attempt to compromise the security of databases, manipulate or steal vital records, or disrupt services through cyberattacks. Robust cybersecurity measures, including encryption, firewalls, intrusion detection systems, and regular security audits, are essential to safeguard sensitive data and ensure the continuity of civil registration operations. Secondly, the issue of identity theft poses a significant challenge to civil registration security. Fraudulent practices, such as the creation of fake identities or the alteration of existing records, can undermine the trustworthiness of the system and lead to the misallocation of resources. The implementation of identity verification mechanisms, such as biometrics or unique identifiers, can enhance the accuracy and integrity of civil registration data while reducing the risk of identity fraud. Thirdly, ensuring the privacy and confidentiality of individuals' personal information is critical in civil registration systems. With the increasing digitization and interconnectedness of data, there is a heightened risk of unauthorized access or data breaches. Strong data protection regulations, robust access controls, and encryption techniques can help mitigate these risks, fostering public trust and confidence in civil registration processes. Moreover, the challenge of inclusivity must be addressed to ensure the effectiveness and reliability of civil registration systems. Marginalized populations, including refugees, migrants, and those residing in remote areas, may face barriers in accessing civil registration services, leaving them vulnerable to identity-related challenges. Deploying mobile registration units, leveraging innovative technologies, and promoting community engagement are strategies that can improve inclusivity and extend the benefits of civil registration to all individuals.

Keywords: Civil Registration; Attacks; Privacy; Security; Vital Information

1. Introduction

Civil registration systems play a crucial role in capturing and managing vital events such as births, deaths, marriages, and divorces as shown in Figure 1. However, these systems are not immune to security and privacy issues, especially in today's digital landscape. The five key areas of concern regarding civil registration security and privacy include cyber-security threats, identity theft and fraud, privacy concerns, inclusivity and marginalized populations, legal and policy frameworks [1]-[6].

*Corresponding author: Peter Kennedy Okoth

With the digitization of civil registration processes, the risk of cyber threats has increased. Malicious actors may attempt to gain unauthorized access to databases, manipulate records, or disrupt services through cyberattacks [7]-[9]. Such incidents can lead to data breaches, compromise the integrity of vital records, and undermine public trust. Robust cybers-ecurity measures, including regular security audits, strong access controls, encryption techniques, and employee training on cyber hygiene, are essential to protect sensitive data and maintain the security of civil registration systems [10], [11]. According to [12], civil registration systems hold personal information that can be exploited for identity theft and fraudulent activities. Unauthorized individuals may attempt to create fake identities or alter existing records to gain undeserved benefits or evade legal obligations. Identity verification mechanisms, such as biometrics (e.g., fingerprints or facial recognition) and unique identifiers, can enhance the accuracy and integrity of civil registration data, reducing the risk of identity theft and fraud [13]-[16].

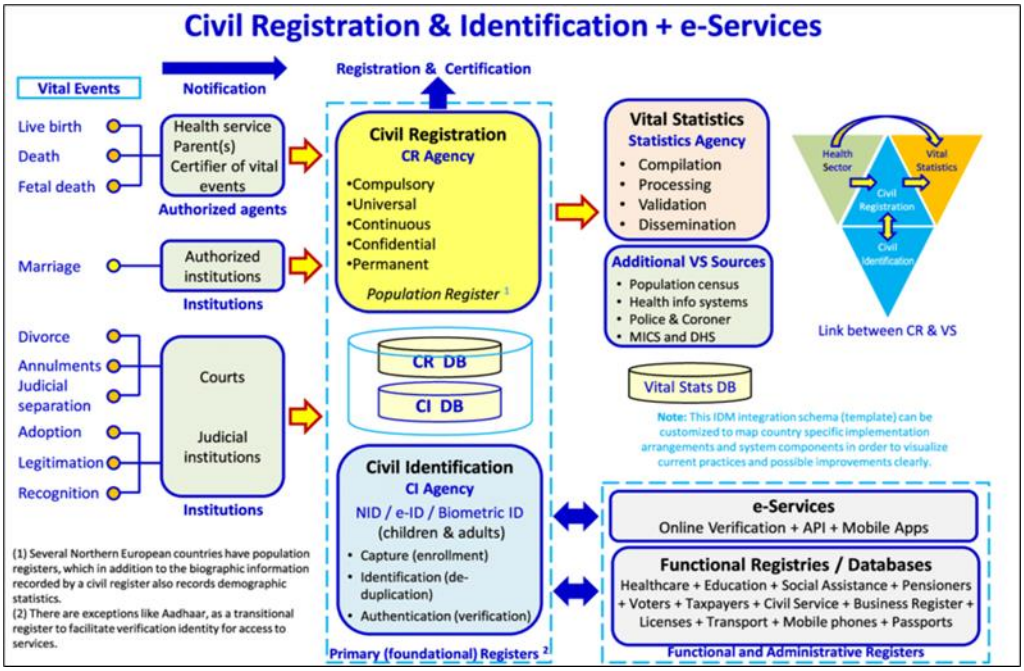

Figure 1 Civil registration procedures

In their study, authors in [17] explain that civil registration involves the collection and storage of individuals' personal information. Safeguarding privacy is crucial to maintain public trust and comply with data protection regulations. However, the increasing digitization and interconnectedness of data pose challenges to privacy [18], [19]. There is a need for robust data protection measures, including encryption, anonymization techniques, strict access controls, and clear policies on data sharing and retention [20], [21]. Governments should prioritize privacy considerations to ensure individuals' personal information is adequately protected. Civil registration systems must be inclusive and ensure that all individuals, including marginalized populations, can access and benefit from their services. However, certain groups, such as refugees, migrants, or individuals living in remote areas, may face barriers in accessing civil registration services [22]-[24]. Lack of registration can lead to exclusion from basic services and legal protections. To address this issue, governments should consider deploying mobile registration units, leveraging innovative technologies (such as mobile applications or remote registration systems), and engaging with communities to improve accessibility and inclusivity. According to [25], a robust legal and policy framework is essential to address security and privacy issues in civil registration systems. Clear guidelines on data protection, security protocols, and the handling of sensitive information should be established [26]-[31]. Governments should also ensure compliance with relevant international standards and regulations [32], [33]. Additionally, public awareness campaigns can educate individuals about their rights regarding the collection, use, and protection of their personal data [34]-[36].

It is clear that civil registration systems face various security and privacy challenges in the digital era [37]. Governments must implement comprehensive measures to address cybersecurity threats, prevent identity theft and fraud, safeguard privacy, promote inclusivity, and establish strong legal and policy frameworks. By prioritizing these concerns, civil registration systems can maintain the accuracy, integrity, and trustworthiness of vital records while respecting individuals' privacy rights and ensuring the accessibility of services to all.

1.1. Common risks in civil registration systems

Civil registration systems, like any other digital systems, are vulnerable to various security risks [38]. Some common security risks in civil registration systems include unauthorized access, data breaches, insider threats, Denial of Service (DoS) attacks, malware and ransomware attacks, social engineering, inadequate security measures, lack of data protection and privacy measures, inadequate disaster recovery and business continuity plans, inclusivity and accessibility challenges. Table 1 presents a summary of these risks and their descriptions.

Table 1 Common risks in civil registration systems

Risk	Explanation
Unauthorized access	One of the primary security risks in civil registration systems is unauthorized access to the system and its databases [39], [40]. If proper access controls and authentication mechanisms are not in place, malicious actors can gain unauthorized access to sensitive data, manipulate records, or disrupt system operations [41], [42].
Data breaches	Data breaches occur when sensitive information is accessed, disclosed, or stolen by unauthorized individuals. This can happen due to system vulnerabilities, weak security measures, or human error [43]-[46]. Data breaches can lead to identity theft, fraud, and misuse of personal information.
Social engineering	Social engineering involves manipulating individuals or exploiting their trust to gain unauthorized access to systems or sensitive information [47]-[51]. Techniques such as phishing emails, impersonation, or pretexting can deceive individuals into providing access credentials or divulging confidential information.
Insider threats	Insider threats involve individuals who have authorized access to the system and intentionally misuse or disclose sensitive data [52]-[56]. This can occur due to personal motivations, such as financial gain or revenge, or due to negligence in following security protocols.
Denial of Service (DoS) attacks	DoS attacks aim to disrupt or disable the civil registration system by overwhelming it with excessive requests or flooding it with malicious traffic [57]-[61]. These attacks can render the system unavailable, preventing legitimate users from accessing services or causing delays in processing vital events.
Inadequate security measures	Weak or outdated security measures pose significant risks to civil registration systems. This includes using weak passwords, not implementing encryption protocols, neglecting security updates and patches, or inadequate physical security measures for servers and infrastructure [62]-[66].
Malware and ransomware attacks	Malware, including viruses, worms, or ransomware, can infect civil registration systems and compromise data integrity and system functionality [67]-[71]. Ransomware attacks encrypt data and demand ransom for its release, causing significant disruptions and potential data loss.
Inclusivity and accessibility challenges	Inadequate security measures or complex registration processes can hinder accessibility and inclusivity, particularly for marginalized populations [72]. This may result in exclusion from essential services or the creation of counterfeit identities.
Lack of data protection and privacy measures	Insufficient data protection measures can result in privacy breaches and violations of individuals' rights [73]-[76]. If personal data is not adequately anonymized, encrypted, or protected, it can be misused or accessed by unauthorized entities.
Inadequate disaster recovery and business continuity plans	Natural disasters, system failures, or cyberattacks can disrupt civil registration systems. Inadequate disaster recovery and business continuity plans can lead to data loss, service interruptions, and extended downtime, impacting the integrity and availability of vital records [77]-[80].

Addressing these security risks requires implementing robust cybersecurity measures, including strong access controls, encryption protocols, regular security audits, user awareness and training programs, and disaster recovery plans [81].

It is essential to prioritize security and privacy in the design, implementation, and maintenance of civil registration systems to ensure the integrity, confidentiality, and availability of vital records while protecting individuals' privacy rights.

1.2. Threats and vulnerabilities in civil registration systems

Civil registration systems are critical for capturing and maintaining accurate and up-to-date records of vital events such as births, deaths, marriages, and divorces [82]. These systems play a crucial role in providing legal identity, establishing citizenship, and facilitating access to various rights and services. However, like any other information system, civil registration systems are susceptible to threats and vulnerabilities that can undermine their integrity and compromise the accuracy and security of the data they hold [83]-[85]. As shown in Figure 2, some common threats and vulnerabilities associated with civil registration systems include unauthorized access, data breaches, insider threats, inadequate authentication and authorization [86], system and software vulnerabilities, social engineering attacks, lack of data integrity checks, physical security risks, lack of redundancy and backup, lack of awareness and training.

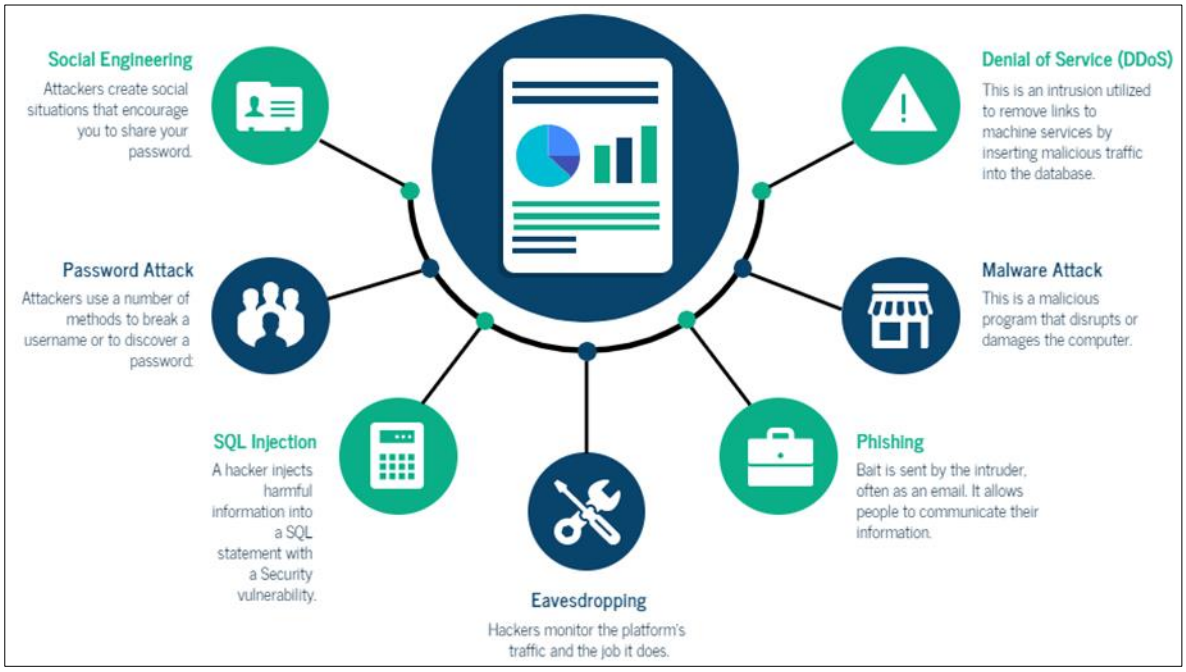

Figure 2 Typical civil registration attacks

According to [87], unauthorized individuals may gain access to the civil registration system and manipulate or tamper with records, leading to inaccuracies or fraudulent activities. Civil registration systems store vast amounts of personal information, including sensitive data such as names, dates of birth, addresses, and sometimes even biometric data. A data breach can expose this information, leading to identity theft, fraud, and other forms of misuse. On the other hand, malicious insiders, such as employees or contractors with authorized access to the system, can abuse their privileges and compromise the integrity of the civil registration system [88]-[91]. They may manipulate records, leak sensitive information, or cause other types of harm. In addition, weak authentication mechanisms and insufficient authorization controls can allow unauthorized individuals to gain access to the system or perform actions beyond their privileges.

Researchers in [92] discuss that civil registration systems are often supported by complex software applications and databases. If these systems are not regularly patched and updated, they can become vulnerable to exploitation by attackers who can exploit software vulnerabilities to gain unauthorized access or disrupt the system [93]-[96]. On the other hand, attackers may attempt to deceive or manipulate individuals within the civil registration system, such as registration officers or system administrators, into revealing sensitive information or granting unauthorized access. In addition, if there are no proper checks and controls in place to ensure the accuracy and integrity of the data entered into the civil registration system, errors or intentional manipulations can occur, leading to incorrect records and compromised system reliability [97]-[101]. Regarding physical security risks, physical infrastructure such as data centers or registration offices may be vulnerable to theft, vandalism, natural disasters, or other physical risks that can lead to loss or damage to the system and its data [102]-[106]. According to [107], failure to implement proper data backup and redundancy measures can result in data loss in the event of hardware failures, natural disasters, or other

disruptions. On the other hand, insufficient awareness among system users about potential threats and vulnerabilities, along with inadequate training on best practices for security and data protection, can increase the risk of security breaches [108]-[110].

To mitigate these threats and vulnerabilities, it is crucial to implement robust security measures, such as strong authentication and access controls, regular system updates and patches, encryption of sensitive data, employee awareness training, and disaster recovery plans [111]. Additionally, conducting regular security audits and risk assessments can help identify and address potential weaknesses in civil registration systems.

1.3. Countermeasures against security breaches in civil registration systems

To safeguard civil registration systems against security and privacy breaches, it is important to implement a comprehensive set of countermeasures as shown in Figure 3. Some effective strategies and practices to mitigate the civil registration systems risks are described in Table 2.

Table 2 Countermeasures against security breaches in civil registration systems

Countermeasures	Descriptions
Access control	Implement strong authentication mechanisms, such as multi-factor authentication, to ensure that only authorized personnel can access the system. Use robust password policies and regularly review and revoke access rights for former employees or contractors [112]-[116]. Apply the principle of least privilege, granting users only the permissions necessary to perform their tasks.
Physical security measures	Implement physical security measures to protect the infrastructure hosting the civil registration system, such as secure access controls, surveillance systems, and alarms [117]-[121]. Regularly assess and address physical security risks, including disaster recovery and business continuity planning.
Regular system updates and patching	Keep the civil registration system and its supporting software applications up to date with the latest security patches and updates. Regularly apply security patches to address known vulnerabilities and stay protected against emerging threats [122]-[126].
Encryption and data protection	Encrypt sensitive data both in transit and at rest. Utilize encryption protocols and algorithms to protect data from unauthorized access or interception. Implement access controls to restrict data access based on user roles and responsibilities [127]-[131]. Regularly back up data and maintain secure off-site backups.
Privacy by design	Incorporate privacy-enhancing features and practices into the design and development of the civil registration system. Implement privacy principles such as data minimization, purpose limitation, and user consent [132]-[136]. Conduct privacy impact assessments to identify and address privacy risks.
Employee awareness and training	Conduct regular security awareness training programs for employees, emphasizing the importance of data privacy, security best practices, and the potential risks associated with social engineering attacks [137-[140]. Teach employees how to identify and report suspicious activities promptly.
Security audits and assessments	Conduct regular security audits and assessments to identify vulnerabilities and gaps in the system's security. Perform penetration testing to simulate attacks and identify potential weaknesses [141]-[146]. Implement intrusion detection and prevention systems to detect and respond to security incidents in real-time.
Compliance with privacy regulations	Stay informed and compliant with relevant privacy regulations and data protection laws. Understand the legal requirements regarding the collection, storage, and processing of personal data in civil registration systems, and ensure that appropriate measures are in place to meet those obligations [147]-[150].
Vendor security assessment	If the civil registration system relies on third-party vendors or service providers, conduct thorough security assessments to ensure their adherence to security and privacy best practices [151]-[154]. Verify that they have appropriate security controls in place to protect the system and its data [155], [156].

Incident response plan	Develop an incident response plan that outlines the steps to be taken in the event of a security breach or privacy incident [157]-[161]. Establish clear roles and responsibilities for incident response team members and ensure that the plan is regularly reviewed, tested, and updated.

By implementing these countermeasures, civil registration systems can be better protected against security and privacy breaches, ensuring the integrity, confidentiality, and availability of the data they hold.

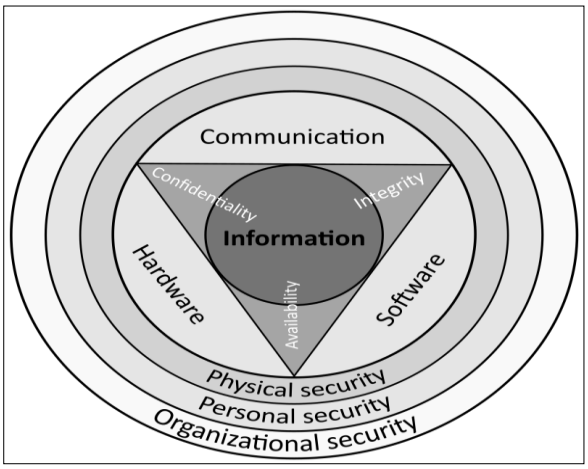

Figure 3 Common attacks countermeasures

Regular monitoring, updating, and improvement of security practices are essential to stay ahead of evolving threats and vulnerabilities.

1.4. Issues with current Countermeasures against security breaches in civil registration systems

While countermeasures are essential for mitigating security and privacy breaches in civil registration systems, there are several challenges that organizations may face in their implementation. These challenges include resource constraints, evolving threat landscape, complexity of systems, user acceptance and compliance, third-party dependencies, legacy systems and technical debt, insider threats and human factors and privacy considerations. According to [162], implementing effective countermeasures requires dedicated resources, including financial investments, skilled personnel, and time. Many organizations, particularly those with limited budgets or capacity, may struggle to allocate sufficient resources to adequately address security and privacy concerns. Authors in [163] explain that threat landscape is constantly evolving, with new attack techniques and vulnerabilities emerging regularly. Keeping up with these changes and adapting countermeasures accordingly can be a significant challenge [164]-[166]. Organizations need to stay informed about the latest security trends and continually update their defenses to address emerging threats effectively. Civil registration systems often comprise complex infrastructures with multiple interconnected components, including databases, software applications, network infrastructure, and user interfaces [167]. Securing such systems requires a holistic approach and a deep understanding of the interdependencies between various components. Ensuring consistent security across the entire system can be challenging, especially if different components are managed by different teams or vendors [168]-[170].

Countermeasures often involve implementing security controls that can impact user experience and workflows [171]-[175]. Users may find security measures cumbersome or time-consuming, leading to potential resistance and non-compliance [176]. Balancing security requirements with user acceptance and adoption is crucial for the effectiveness of countermeasures. Regarding third-Party dependencies, civil registration systems may rely on third-party vendors or service providers for certain functionalities or infrastructure [177]. Managing the security of these external dependencies can be challenging since organizations have limited control over the security practices of third parties [178]-[180]. It is essential to conduct thorough vendor assessments and establish clear contractual agreements to ensure the security and privacy [181] of the system. According to [182], many civil registration systems have been in operation for a long time, and they may be built on outdated technologies or legacy systems. These legacy systems often lack modern security features and may have accumulated technical debt, making it difficult to implement robust countermeasures [183]. Upgrading or replacing such systems can be costly and disruptive.

Regarding insider threats and human factors, countermeasures need to address not only external threats but also internal risks, such as insider threats and human error [184]-[187]. Malicious insiders or negligent employees can circumvent security controls or inadvertently introduce vulnerabilities. Educating and raising awareness among employees about security best practices is crucial but can be challenging to achieve consistently [188]-[193]. As explained in [194], countermeasures aimed at enhancing security may sometimes conflict with privacy requirements. Striking the right balance between security and privacy can be a challenge, as organizations must ensure the protection of personal data while maintaining the integrity and availability of the system.

Overcoming these challenges requires a proactive and multidimensional approach, including ongoing risk assessments, regular training and awareness programs, collaboration with stakeholders, and a commitment to continuous improvement. It is crucial to regularly reassess and adapt countermeasures to address emerging challenges and evolving threats effectively.

1.5. Security models in civil registration systems

Security models in civil registration systems provide a framework for organizing and implementing security measures to protect the system and its data. These models define the structure, components, and principles for establishing a secure environment. The three commonly used security models in civil registration systems are described in Table 3 below.

Table 3 Security models in civil registration systems

Model	Discussion
Confidentiality, Integrity, and Availability (CIA) Model	The CIA model forms the basis of information security. It focuses on three core principles: *Confidentiality*: Ensuring that data and information are only accessible to authorized individuals or entities. This involves measures such as access controls, encryption, and secure communication channels to protect against unauthorized disclosure [195]-[200]. *Integrity*: Guaranteeing the accuracy, consistency, and trustworthiness of data throughout its lifecycle. Measures such as data validation, digital signatures, and audit trails help maintain data integrity and prevent unauthorized modification [201]-[207]. *Availability*: Ensuring that the civil registration system and its services are accessible and operational when needed [208], [209]. Measures like redundant systems, disaster recovery plans, and regular maintenance and monitoring are implemented to minimize downtime and ensure system availability.
Defense-in-depth model	The defense-in-depth model employs multiple layers of security controls to provide comprehensive protection. It assumes that no single security measure is foolproof, so it implements a combination of preventive, detective, and corrective controls at different layers [210], [211]. These layers may include: *Perimeter Security*: Protecting the boundaries of the civil registration system, such as firewalls, intrusion prevention systems, and access controls [212]. *Network Security*: Securing the network infrastructure, including secure protocols, network segmentation, and traffic monitoring. *Host Security*: Implementing security controls on individual servers or endpoints, such as strong authentication, patch management, and malware protection. *Application Security*: Ensuring that software applications within the civil registration system are secure, including secure coding practices, vulnerability assessments, and secure configuration [214]. *Data Security*: Protecting the confidentiality, integrity, and availability of data through encryption, access controls, data backup, and data loss prevention mechanisms [215]. *User Security*: Implementing user-focused security measures, including user awareness training, strong authentication, and user access management [216].
Risk-based security model	The risk-based security model emphasizes identifying and mitigating risks based on their potential impact and likelihood [217]. It involves the following steps:

	Risk Assessment: Identifying and evaluating potential risks and threats to the civil registration system and its data. This includes conducting vulnerability assessments, threat modeling, and risk analysis. *Risk Mitigation*: Implementing security controls and countermeasures based on the identified risks. This involves prioritizing risks, selecting appropriate controls, and implementing security measures to reduce the risk level. *Risk Monitoring and Review*: Continuously monitoring the system for new risks and vulnerabilities, as well as assessing the effectiveness of implemented security measures. Regular reviews and audits help identify gaps and improve security posture over time.

These security models provide a foundation for designing and implementing effective security measures in civil registration systems. However, it's important to tailor these models to the specific context and requirements of the system, considering factors such as the sensitivity of the data, the threat landscape, and applicable regulations and standards.

1.6. Future research prospects in civil registration systems security

Future research in civil registration systems security can focus on several key areas to enhance the protection of sensitive data and mitigate emerging threats. The following are some potential research prospects.

- *Privacy-Preserving Technologies*: Explore and develop advanced techniques for privacy-preserving data management in civil registration systems [218]-[221]. This includes secure data sharing, cryptographic protocols, differential privacy, and secure multi-party computation to balance the need for data security with individual privacy rights.
- *Biometric Security*: Investigate the use of biometric authentication and verification methods to strengthen the security of civil registration systems [222]-[224]. Research can focus on biometric recognition algorithms, anti-spoofing techniques, and secure storage and transmission of biometric data.
- *Blockchain and Distributed Ledger Technology*: Examine the potential applications of blockchain and distributed ledger technology in civil registration systems [225], [226]. Research can explore the use of decentralized and tamper-proof ledgers for securely recording and managing vital events, identity verification, and data integrity.
- *Artificial Intelligence (AI) for Threat Detection*: Investigate the use of AI and machine learning techniques to detect anomalies, patterns, and potential security breaches in civil registration systems [227]-[231]. Research can focus on developing AI-based models [232] for intrusion detection, fraud detection, and predictive analytics to enhance system security.
- *Secure Data Sharing and Interoperability*: Address the challenges of securely sharing data between different civil registration systems and other relevant government or private sector entities [233]-[236]. Research can explore secure data exchange protocols, interoperability standards, and secure data integration techniques while maintaining data privacy and security.
- *Human Factors and User-Centric Security*: Examine the human factors and usability aspects of security in civil registration systems. Research can focus on understanding user behaviors, perceptions, and vulnerabilities to design user-centric security measures, effective [237] training programs, and usable security interfaces.
- *IoT Security*: Investigate the security challenges and vulnerabilities associated with Internet of Things (IoT) devices used in civil registration systems [238]-[240]. Research can focus on securing IoT devices, data transmission, and ensuring the integrity and privacy of IoT-generated data.
- *Threat Intelligence and Sharing*: Explore methodologies for collecting, analyzing, and sharing threat intelligence specific to civil registration systems [241], [242]. Research can focus on developing collaborative platforms and frameworks for sharing security information, best practices, and threat indicators among relevant stakeholders.
- *Security Governance and Policies*: Examine the governance structures, policies, and regulatory frameworks surrounding the security of civil registration systems [243]-[245]. Research can focus on assessing the effectiveness of existing policies, identifying gaps, and proposing guidelines and best practices for security governance.
- *Resilience and Disaster Recovery*: Investigate methods to enhance the resilience and disaster recovery capabilities of civil registration systems [246], [247]. Research can focus on developing robust backup and recovery mechanisms, business continuity planning, and incident response strategies to ensure the system's availability in the face of disruptions.

These research prospects aim to address the evolving security landscape and challenges faced by civil registration systems, paving the way for more secure and reliable systems that protect the integrity and privacy of vital records and personal data.

2. Conclusion

In conclusion, privacy and security issues in civil registration systems are critical concerns that need to be addressed effectively. The sensitivity of the personal data stored in these systems, coupled with the potential impact on individuals' legal identity and access to rights and services, highlights the importance of robust privacy and security measures. Threats such as unauthorized access, data breaches, insider attacks, and system vulnerabilities pose significant risks to the integrity and confidentiality of the data. To mitigate these risks, organizations must implement comprehensive countermeasures that encompass access control, encryption, regular updates, employee training, and physical security measures. Additionally, the ongoing research prospects in the field, including privacy-preserving technologies, biometric security, blockchain, AI, and IoT security, offer promising avenues to strengthen the privacy and security of civil registration systems. By prioritizing privacy and security in the design, implementation, and governance of these systems, we can ensure the protection of personal data and foster trust in civil registration processes, ultimately upholding the rights and welfare of individuals within society.

Compliance with ethical standards

Acknowledgments

Much appreciation to all my colleagues who helped me in one way or the other when developing this manuscript.

References

[1] Garunja, E. (2023). Protection of Privacy and Personal Data in Albania. Croatian and Comparative Public Administration, 23(1), 91-116.

[2] Dar, M. A., & Wani, S. A. (2023). COVID-19, Personal Data Protection and Privacy in India. Asian Bioethics Review, 15(2), 125-140.

[3] Tayyab, M., Marjani, M., Jhanjhi, N. Z., Hashem, I. A. T., Usmani, R. S. A., & Qamar, F. (2023). A Comprehensive Review on Deep Learning Algorithms: Security and Privacy Issues. Computers & Security, 103297.

[4] Thantilage, R. D., Le-Khac, N. A., &Kechadi, M. T. (2023). Healthcare data security and privacy in Data Warehouse architectures. Informatics in Medicine Unlocked, 101270.

[5] Gupta, B. B., Gaurav, A., &Panigrahi, P. K. (2023). Analysis of security and privacy issues of information management of big data in B2B based healthcare systems. Journal of Business Research, 162, 113859.

[6] Nyangaresi, V. O. (2023). Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks, 142, 103117.

[7] Ahmad, H., Dharmadasa, I., Ullah, F., & Babar, M. A. (2023). A Review on C3I Systems' Security: Vulnerabilities, Attacks, and Countermeasures. ACM Computing Surveys, 55(9), 1-38.

[8] Bao, S. P. R. M. B., Bao, E. F. M. B., Bao, M. C. M. B., Dip, G., & Bao, J. C. M. B. (2023). The Irish National Orthopaedic Register Under Cyberattack: What Happened, and What Were the Consequences?.

[9] Mishra, S. (2023). Exploring the Impact of AI-Based Cyber Security Financial Sector Management. Applied Sciences, 13(10), 5875.

[10] Bandari, V. (2023). Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types. International Journal of Business Intelligence and Big Data Analytics, 6(1), 1-11.

[11] Hussien, Z. A., Abdulmalik, H. A., Hussain, M. A., Nyangaresi, V. O., Ma, J., Abduljabbar, Z. A., &Abduljaleel, I. Q. (2023). Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences, 13(2), 691.

[12] Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2023). Towards protecting organisations' data by preventing data theft by malicious insiders. International Journal of Organizational Analysis, 31(3), 875-888.

[13] Kairaldeen, A. R., Abdullah, N. F., Abu-Samah, A., &Nordin, R. (2023). Peer-to-Peer User Identity Verification Time Optimization in IoT Blockchain Network. Sensors, 23(4), 2106.

[14] Sasikumar, A., Vairavasundaram, S., Kotecha, K., Indragandhi, V., Ravi, L., Selvachandran, G., & Abraham, A. (2023). Blockchain-based trust mechanism for digital twin empowered Industrial Internet of Things. Future Generation Computer Systems, 141, 16-27.

[15] Hong, H., & Sun, Z. (2023). Constructing conditional PKEET with verification mechanism for data privacy protection in intelligent systems. The Journal of Supercomputing, 1-19.

[16] Nyangaresi, V. O., & Ma, J. (2022, June). A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In 2022 IEEE World Conference on Applied Intelligence and Computing (AIC) (pp. 416-422). IEEE.

[17] Munoriyarwa, A., & Mare, A. (2023). Mainstreaming Surveillance Through the Biometrification of Everyday Life. In Digital Surveillance in Southern Africa: Policies, Politics and Practices (pp. 141-156). Cham: Springer International Publishing.

[18] Almeida, F., Santos, J. D., & Monteiro, J. A. (2020). The challenges and opportunities in the digitalization of companies in a post-COVID-19 World. IEEE Engineering Management Review, 48(3), 97-103.

[19] Paul, M., Maglaras, L., Ferrag, M. A., &AlMomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. ICT Express.

[20] Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (2018, December). Privacy issues and data protection in big data: a case study analysis under GDPR. In 2018 IEEE International Conference on Big Data (Big Data) (pp. 5027-5033). IEEE.

[21] Al Sibahee, M. A., Nyangaresi, V. O., Ma, J., &Abduljabbar, Z. A. (2022, July). Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. In IoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings (pp. 3-18). Cham: Springer International Publishing.

[22] Chudnovsky, M., &Peeters, R. (2022). A cascade of exclusion: Administrative burdens and access to citizenship in the case of Argentina's national identity document. International Review of Administrative Sciences, 88(4), 1068-1085.

[23] Razali, R. M., Duraisingam, T. J., & Lee, N. N. X. (2022). Digitalisation of birth registration system in Malaysia: Boon or bane for the hard-to-reach and marginalised?. Journal of Migration and Health, 6, 100137.

[24] Erasmus, P. (2022). Statelessness, the Right to Health, Policy, and Case Law. Systems Thinking for Global Health: How can systems-thinking contribute to solving key challenges in Global Health?, 293.

[25] McClain, S. N., Bruch, C., Daly, E., May, J., Hamada, Y., Maekawa, M., ... &Tsiokanou, G. (2022). Migration with dignity: A legal and policy framework. Journal of Disaster Research, 17(3), 292-300.

[26] Nyangaresi, V. O. (2023). Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. In Computer Vision and Robotics: Proceedings of CVR 2022 (pp. 503-516). Singapore: Springer Nature Singapore.

[27] Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., &Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). Applied Sciences, 12(4), 1927.

[28] Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. SN Computer Science, 3(2), 127.

[29] Gürsoy, G., Li, T., Liu, S., Ni, E., Brannon, C. M., & Gerstein, M. B. (2022). Functional genomics data: privacy risk assessment and technological mitigation. Nature Reviews Genetics, 23(4), 245-258.

[30] Rizi, M. H. P., & Seno, S. A. H. (2022). A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. Internet of Things, 100584.

[31] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31;47(6).

[32] Aksoy, T., & Aksoy, L. (2020). Increasing importance of internal control in the light of global developments, national and international standards and regulations. SayıştayDergisi, (118), 9-40.

[33] Salguero-Caparrós, F., Pardo-Ferreira, M. D. C., Martínez-Rojas, M., & Rubio-Romero, J. C. (2020). Management of legal compliance in occupational health and safety. A literature review. Safety science, 121, 111-118.

[34] Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. Telematics and Informatics, 35(6), 1770-1780.

[35] Prince, C., Omrani, N., Maalaoui, A., Dabic, M., & Kraus, S. (2021). Are we living in surveillance societies and is privacy an illusion? An empirical study on privacy literacy and privacy concerns. IEEE Transactions on Engineering Management.

[36] Nyangaresi, V. O., &Moundounga, A. R. A. (2021, September). Secure data exchange scheme for smart grids. In 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) (pp. 312-316). IEEE.

[37] Verma, A., Khanna, A., Agrawal, A., Darwish, A., &Hassanien, A. E. (2019). Security and privacy in smart city applications and services: Opportunities and challenges. Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments, 1-15.

[38] Ball, J., Butt, L., & Beazley, H. (2017). Birth registration and protection for children of transnational labor migrants in Indonesia. Journal of Immigrant & Refugee Studies, 15(3), 305-325.

[39] Vora, J., DevMurari, P., Tanwar, S., Tyagi, S., Kumar, N., &Obaidat, M. S. (2018, July). Blind signatures based secured e-healthcare system. In 2018 International conference on computer, information and telecommunication systems (CITS) (pp. 1-5). IEEE.

[40] Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. (2020). A review of cybersecurity incidents in the water sector. Journal of Environmental Engineering, 146(5), 03120003.

[41] Abduljabbar, Z. A., OmolloNyangaresi, V., Al Sibahee, M. A., Ghrabat, M. J. J., Ma, J., QaysAbduljaleel, I., &Aldarwish, A. J. (2022). Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks, 11(3), 55.

[42] Telo, J. (2023). Smart City Security Threats and Countermeasures in the Context of Emerging Technologies. International Journal of Intelligent Automation and Computing, 6(1), 31-45.

[43] Barona, R., & Anita, E. M. (2017, April). A survey on data breach challenges in cloud computing security: Issues and threats. In 2017 International conference on circuit, power and computing technologies (ICCPCT) (pp. 1-8). IEEE.

[44] Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. Journal of medical systems, 43, 1-12.

[45] Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020, May). Healthcare data breaches: insights and implications. In Healthcare (Vol. 8, No. 2, p. 133). MDPI.

[46] Nyangaresi, V. O. (2022, June). Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In 2022 4th Global Power, Energy and Communication Conference (GPECOM) (pp. 427-432). IEEE.

[47] Vrhovec, S., Bernik, I., &Markelj, B. (2023). Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign. Computers & Security, 125, 103038.

[48] Pethers, B., & Bello, A. (2023). Role of Attention and Design Cues for Influencing Cyber-Sextortion Using Social Engineering and Phishing Attacks. Future Internet, 15(1), 29.

[49] Campbell, C. C. (2019). Solutions for counteracting human deception in social engineering attacks. Information Technology & People, 32(5), 1130-1152.

[50] Finch, J. (2022). Social policy, social engineering and the family in the 1990s. In The Goals of Social Policy (pp. 160-169). Routledge.

[51] Abduljabbar, Z. A., Nyangaresi, V. O., Ma, J., Al Sibahee, M. A., Khalefa, M. S., & Honi, D. G. (2022, September). MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. In Future Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings (pp. 16-36). Cham: Springer International Publishing.

[52] Marbut, A. R., & Harms, P. D. (2023). Fiends and Fools: A Narrative Review and Neo-socioanalytic Perspective on Personality and Insider Threats. Journal of Business and Psychology, 1-18.

[53] Pal, P., Chattopadhyay, P., &Swarnkar, M. (2023). Temporal feature aggregation with attention for insider threat detection from activity logs. Expert Systems with Applications, 224, 119925.

[54] Singh, M., Mehtre, B. M., Sangeetha, S., &Govindaraju, V. (2023). User Behaviour based Insider Threat Detection using a Hybrid Learning Approach. Journal of Ambient Intelligence and Humanized Computing, 14(4), 4573-4593.

[55] AlSlaiman, M., Salman, M. I., Saleh, M. M., & Wang, B. (2023). Enhancing false negative and positive rates for efficient insider threat detection. Computers & Security, 126, 103066.

[56] Nyangaresi, V. O., &Ogundoyin, S. O. (2021, October). Certificate based authentication scheme for smart homes. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) (pp. 202-207). IEEE.

[57] Cheng, F., Liang, H., Niu, B., Zhao, N., & Zhao, X. (2023). Adaptive neural self-triggered bipartite secure control for nonlinear MASs subject to DoS attacks. Information Sciences, 631, 256-270.

[58] Zhao, N., Zhao, X., Chen, M., Zong, G., & Zhang, H. (2023). Resilient distributed event-triggered platooning control of connected vehicles under denial-of-service attacks. IEEE Transactions on Intelligent Transportation Systems.

[59] Salmi, S., &Oughdir, L. (2023). Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network. Journal of Big Data, 10(1), 1-25.

[60] Wen, G., Wang, P., Lv, Y., Chen, G., & Zhou, J. (2023). Secure consensus of multi-agent systems under denial-of-service attacks. Asian Journal of Control, 25(2), 695-709.

[61] Nyakomitta, P. S., Nyangaresi, V. O., &Ogara, S. O. (2021). Efficient authentication algorithm for secure remote access in wireless sensor networks. Journal of Computer Science Research, 3(4), 43-50.

[62] Altulaihan, E. A., Alismail, A., &Frikha, M. (2023). A Survey on Web Application Penetration Testing. Electronics, 12(5), 1229.

[63] Addobea, A. A., Li, Q., ObiriJr, I. A., & Hou, J. (2023). Secure multi-factor access control mechanism for pairing blockchains. Journal of Information Security and Applications, 74, 103477.

[64] Softić, J., &Vejzović, Z. (2023, March). Impact of Vulnerability Assesment and Penetration Testing (VAPT) on Operating System Security. In 2023 22nd International Symposium Infoteh-Jahorina (INFOTEH) (pp. 1-6). IEEE.

[65] Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2023). Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. Internet of Things and Cyber-Physical Systems.

[66] Nyangaresi, V. O., &Morsy, M. A. (2021, September). Towards privacy preservation in internet of drones. In 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) (pp. 306-311). IEEE.

[67] Gorment, N. Z., Selamat, A., Cheng, L. K., &Krejcar, O. (2023). Machine Learning Algorithm for Malware Detection: Taxonomy, Current Challenges and Future Directions. IEEE Access.

[68] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, 12(6), 1333.

[69] SANDU, E. Ş. (2023, May). Prevention of Widespread Ransomware Cyber-Attacks through the SEAP Platform. In Proceedings of the International Conference on Cybersecurity and Cybercrime-2023 (pp. 230-240). AsociatiaRomanapentruAsigurareaSecuritatiiInformatiei.

[70] Möller, D. P. (2023). Threats and Threat Intelligence. In Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices (pp. 71-129). Cham: Springer Nature Switzerland.

[71] Alsamhi, S. H., Shvetsov, A. V., Kumar, S., Shvetsova, S. V., Alhartomi, M. A., Hawbani, A., ... &Nyangaresi, V. O. (2022). UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones, 6(7), 154.

[72] Balasamy, K., Krishnaraj, N., Ramprasath, J., & Ramprakash, P. (2022). A secure framework for protecting clinical data in medical IoT environment. Smart healthcare system design: security and privacy aspects, 203-234.

[73] Rosenfeld, L., Torous, J., &Vahia, I. V. (2017). Data security and privacy in apps for dementia: an analysis of existing privacy policies. The American Journal of Geriatric Psychiatry, 25(8), 873-877.

[74] Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. Future Generation Computer Systems, 98, 660-671.

[75] Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. Telematics and Informatics, 34(4), 157-170.

[76] Nyangaresi, V. O., & Petrovic, N. (2021, July). Efficient PUF based authentication protocol for internet of drones. In 2021 International Telecommunications Conference (ITC-Egypt) (pp. 1-4). IEEE.

[77] Vanichchinchai, A. (2023). The influences of organizational contexts on business continuity management. Business Process Management Journal, 29(1), 100-115.

[78] Chizwina, S., &Ngulube, P. (2023). Disaster risk identification and business continuity planning in community libraries in the North West Province in South Africa. South African Journal of Libraries and Information Science, 89(1), 1-9.

[79] McAliney, P. J., Albertini, G. J., &Ramsaywak, S. D. (2023). Incidence Response, Disaster Recovery, and Business Continuity Planning: Their Role in an Institution's Risk Management Plan. In Handbook of Research on Current Trends in Cybersecurity and Educational Technology (pp. 37-59). IGI Global.

[80] Vanichchinchai, A. (2023). Links between components of business continuity management: an implementation perspective. Business Process Management Journal, (ahead-of-print).

[81] Mohammad, Z., Nyangaresi, V., &Abusukhon, A. (2021, July). On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In 2021 International Conference on Information Technology (ICIT) (pp. 320-325). IEEE.

[82] Saikia, N., Kumar, K., & Das, B. (2023). Death registration coverage 2019–2021, India. Bulletin of the World Health Organization, 101(2), 102.

[83] Toapanta, S. M. T., Saá, I. F. M., Quimi, F. G. M., & Gallegos, L. E. M. (2019). An approach to vulnerabilities, threats and risk in voting systems for popular elections in Latin America. Adv. Sci. Technol. Eng. Syst. J, 4(3), 106-116.

[84] Sheik, A. T., Maple, C., Epiphaniou, G., &Atmaca, U. I. (2021). A comparative study of cyber threats on evolving digital identity systems.

[85] Andrew, L. (2020). The vulnerability of vital systems: how'criticalinfrastructure'became a security problem. In Securing 'the Homeland' (pp. 17-39). Routledge.

[86] Nyangaresi, V. O. (2023, February). Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. In Proceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 (pp. 797-816). Singapore: Springer Nature Singapore.

[87] Hill, P., & Lin, Y. J. (2022). Evaluation of Trust Worthiness of State and County Government Websites. Accessed: Apr, 21.

[88] Zhang, Y., & Smith, T. (2023). The impact of customer firm data breaches on the audit fees of their suppliers. International Journal of Accounting Information Systems, 50, 100628.

[89] Chu, S. (2023). The role of enterprise systems standardization on data breach occurrence (Doctoral dissertation, University of British Columbia).

[90] Li, Y., &Mamon, R. (2023). Modelling health-data breaches with application to cyber insurance. Computers & Security, 124, 102963.

[91] Abduljabbar, Z. A., Abduljaleel, I. Q., Ma, J., Al Sibahee, M. A., Nyangaresi, V. O., Honi, D. G., ... & Jiao, X. (2022). Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access, 10, 26257-26270.

[92] Mainz, J., Hess, M. H., & Johnsen, S. P. (2019). The Danish unique personal identifier and the Danish Civil Registration System as a tool for research and quality improvement. International Journal for Quality in Health Care, 31(9), 717-720.

[93] Jenkins, A., Kalligeros, P., Vaniea, K., & Wolters, M. K. (2020, September). "Anyone Else Seeing this Error?": Community, System Administrators, and Patch Information. In 2020 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 105-119). IEEE.

[94] Li, F., Rogers, L., Mathur, A., Malkin, N., & Chetty, M. (2019, November). Keepers of the machines: examining how system administrators manage software updates. In Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security (pp. 273-288). USENIX Association.

[95] Kitchin, R., & Dodge, M. (2020). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. In Smart Cities and Innovative Urban Technologies (pp. 47-65). Routledge.

[96] Al Sibahee, M. A., Abdulsada, A. I., Abduljabbar, Z. A., Ma, J., Nyangaresi, V. O., & Umran, S. M. (2021). Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences, 11(24), 12040.

[97] McCartney, C. (2015). Forensic data exchange: Ensuring integrity. Australian Journal of Forensic Sciences, 47(1), 36-48.

[98] Shen, X., Lu, Y., Zhang, Y., Liu, X., & Zhang, L. (2022). An Innovative Data Integrity Verification Scheme in the Internet of Things assisted information exchange in transportation systems. Cluster Computing, 25(3), 1791-1803.

[99] Pasdar, A., Lee, Y. C., & Dong, Z. (2023). Connect API with blockchain: A survey on blockchain oracle implementation. ACM Computing Surveys, 55(10), 1-39.

[100] Kartoglu, U., & Ames, H. (2022). Ensuring quality and integrity of vaccines throughout the cold chain: the role of temperature monitoring. Expert Review of Vaccines, 21(6), 799-810.

[101] Nyangaresi, V. O. (2021). A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. In the 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612).

[102] Iaiani, M., Tugnoli, A., Cozzani, V., Reniers, G., & Yang, M. (2023). A Bayesian-network approach for assessing the probability of success of physical security attacks to offshore Oil&Gas facilities. Ocean Engineering, 273, 114010.

[103] Li, G., Ren, L., Fu, Y., Yang, Z., Adetola, V., Wen, J., ... & O'Neill, Z. (2023). A critical review of cyber-physical security for building automation systems. Annual Reviews in Control.

[104] Progoulakis, I., Nikitakos, N., Dalaklis, D., Christodoulou, A., Dalaklis, A., & Yaacob, R. (2023). Digitalization and cyber physical security aspects in maritime transportation and port infrastructure. In Smart Ports and Robotic Systems: Navigating the Waves of Techno-Regulation and Governance (pp. 227-248). Cham: Springer International Publishing.

[105] Gooren, J. (2023). The logic of CPTED for public space or the social potential of physical security. Crime, Law and Social Change, 79(4), 417-436.

[106] Hussain, M. A., Hussien, Z. A., Abduljabbar, Z. A., Ma, J., Al Sibahee, M. A., Hussain, S. A., Nyangaresi V.O., & Jiao, X. (2022). Provably throttling SQLI using an enciphering query and secure matching. Egyptian Informatics Journal, 23(4), 145-162.

[107] Smolarz, A., Lezhniuk, P., Kudrya, S., Komar, V., Lysiak, V., Hunko, I., ... &Orazbekov, Z. (2023). Increasing Technical Efficiency of Renewable Energy Sources in Power Systems. Energies, 16(6), 2828.

[108] Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. Heliyon.

[109] Douha, N. G. Y. R., Renaud, K., Taenaka, Y., &Kadobayashi, Y. (2023). Smart home cybersecurity awareness and behavioral incentives. Information & Computer Security.

[110] Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. Technology in Society, 102258.

[111] Nyangaresi, V. O., &Alsamhi, S. H. (2021, October). Towards secure traffic signaling in smart grids. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) (pp. 196-201). IEEE.

[112] Iqbal, W., Abbas, H., Deng, P., Wan, J., Rauf, B., Abbas, Y., & Rashid, I. (2023). ALAM: Anonymous lightweight authentication mechanism for SDN enabled smart homes. Journal of Network and Computer Applications, 103672.

[113] Nita, S. L., &Mihailescu, M. I. (2023). Elliptic Curve-Based Query Authentication Protocol for IoT Devices Aided by Blockchain. Sensors, 23(3), 1371.

[114] Ahmad, M. O., Tripathi, G., Siddiqui, F., Alam, M. A., Ahad, M. A., Akhtar, M. M., &Casalino, G. (2023). BAuth-ZKP—A Blockchain-Based Multi-Factor Authentication Mechanism for Securing Smart Cities. Sensors, 23(5), 2757.

[115] Kang, Y., Kanwal, S., Liu, B., & Zhang, D. (2023). Ghost key distribution under mutual authentication mechanism. Information Sciences, 640, 119025.

[116] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[117] Al-Bkree, M. (2023). Managing the cyber-physical security for unmanned aerial vehicles used in perimeter surveillance. International Journal of Innovative Research and Scientific Studies, 6(1), 164-173.

[118] Ashok, K., &Gopikrishnan, S. (2023). Statistical Analysis of Remote Health Monitoring Based IoT Security Models & Deployments From a Pragmatic Perspective. IEEE Access, 11, 2621-2651.

[119] Azhari, D. W., &Asbari, M. (2023). General Control of Information Systems. Journal of Information Systems and Management (JISMA), 2(2), 8-11.

[120] Farraj, A. (2023, February). Coordinated Security Measures for Industrial IoT Against Eavesdropping. In 2023 IEEE Texas Power and Energy Conference (TPEC) (pp. 1-5). IEEE.

[121] Nyangaresi, V. O. (2022). Terminal independent security token derivation scheme for ultra-dense IoT networks. Array, 15, 100210.

[122] Kioskli, K., Fotis, T., Nifakos, S., &Mouratidis, H. (2023). The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. Applied Sciences, 13(6), 3410.

[123] George, A. S., &Sagayarajan, S. (2023). Securing Cloud Application Infrastructure: Understanding the Penetration Testing Challenges of IaaS, PaaS, and SaaS Environments. Partners Universal International Research Journal, 2(1), 24-34.

[124] Senanayake, J., Kalutarage, H., Al-Kadri, M. O., Petrovski, A., &Piras, L. (2023). Android source code vulnerability detection: a systematic literature review. ACM Computing Surveys, 55(9), 1-37.

[125] Hong, S., Xu, L., Huang, J., Li, H., Hu, H., & Gu, G. (2023). SysFlow: Toward a Programmable Zero Trust Framework for System Security. IEEE Transactions on Information Forensics and Security, 18, 2794-2809.

[126] Mutlaq, K. A. A., Nyangaresi, V. O., Omar, M. A., &Abduljabbar, Z. A. (2022, October). Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. In Applied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings (pp. 46-64). Cham: Springer Nature Switzerland.

[127] Fan, C. I., Shie, C. H., Tseng, Y. F., & Huang, H. C. (2023). An Efficient Data Protection Scheme Based on Hierarchical ID-Based Encryption for MQTT. ACM Transactions on Sensor Networks, 19(3), 1-21.

[128] Rupa, C., & Shah, M. A. (2023). Novel secure data protection scheme using Martino homomorphic encryption. Journal of Cloud Computing, 12(1), 1-12.

[129] Zhang, X., Mu, D., & Zhao, J. (2023). Attribute-based keyword search encryption for power data protection. High-Confidence Computing, 100115.

[130] Qiu, M., & Gao, X. (2023, May). Multi-level Encryption for Agricultural Data Protection. In 2023 IEEE 9th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS) (pp. 141-146). IEEE.

[131] Nyangaresi, V. O. (2022). A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science, 3(5), 364.

[132] Alkhariji, L., De, S., Rana, O., & Perera, C. (2023). Semantics-based privacy by design for Internet of Things applications. Future Generation Computer Systems, 138, 280-295.

[133] Semantha, F. H., Azam, S., Shanmugam, B., & Yeo, K. C. (2023). PbDinEHR: A Novel Privacy by Design Developed Framework Using Distributed Data Storage and Sharing for Secure and Scalable Electronic Health Records Management. Journal of Sensor and Actuator Networks, 12(2), 36.

[134] De Brouwer, M., Steenwinckel, B., Fang, Z., Stojchevska, M., Bonte, P., De Turck, F., ... &Ongenae, F. (2023). Context-aware query derivation for IoT data streams with DIVIDE enabling privacy by design. Semantic Web, (Preprint), 1-49.

[135] Mohsen, M., Rizk, H., & Youssef, M. (2023). Privacy-preserving by design: Indoor positioning system using wi-fi passive tdoa. arXiv preprint arXiv:2306.02211.

[136] Abood, E. W., Hussien, Z. A., Kawi, H. A., Abduljabbar, Z. A., Nyangaresi, V. O., Ma, J., ... & Ahmad, S. (2023). Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708), 13(1).

[137] Farid, G., Warraich, N. F., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). Journal of Information Science, 01655515231160026.

[138] Saeed, S. (2023). Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. Sustainability, 15(7), 6019.

[139] Yazdanmehr, A., Li, Y., & Wang, J. (2023). Employee responses to information security related stress: Coping and violation intention. Information Systems Journal.

[140] Frank, M., Jaeger, L., &Ranft, L. M. (2023). Using contextual factors to predict information security overconfidence: A machine learning approach. Computers & Security, 125, 103046.

[141] Nyangaresi, V. O. (2021). Hardware assisted protocol for attacks prevention in ad hoc networks. In Emerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 (pp. 3-20). Springer International Publishing.

[142] Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., &Klepacki, B. (2020). Information security assessment in public administration. Computers & Security, 90, 101709.

[143] Thompson, N., Mullins, A., &Chongsutakawewong, T. (2020). Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand. Government Information Quarterly, 37(1), 101408.

[144] Grieco, G., Song, W., Cygan, A., Feist, J., &Groce, A. (2020, July). Echidna: effective, usable, and fast fuzzing for smart contracts. In Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis (pp. 557-560).

[145] Upadhyay, D., &Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. Computers & Security, 89, 101666.

[146] Abood, E. W., Abdullah, A. M., Al Sibahe, M. A., Abduljabbar, Z. A., Nyangaresi, V. O., Kalafy, S. A. A., &Ghrabta, M. J. J. (2022). Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics, 11(1), 185-194.

[147] Anderson, C., Baskerville, R., & Kaul, M. (2023). Managing compliance with privacy regulations through translation guardrails: A health information exchange case study. Information and Organization, 33(1), 100455.

[148] Johnson, G. A., Shriver, S. K., & Goldberg, S. G. (2023). Privacy and market concentration: intended and unintended consequences of the GDPR. Management Science.

[149] Bell, A., Nov, O., &Stoyanovich, J. (2023). Think about the stakeholders first! Toward an algorithmic transparency playbook for regulatory compliance. Data & Policy, 5, e12.

[150] Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., &Newe, T. (2023). Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. Sensors, 23(3), 1151.

[151] Nyangaresi, V. O., & Mohammad, Z. (2021, July). Privacy preservation protocol for smart grid networks. In 2021 International Telecommunications Conference (ITC-Egypt) (pp. 1-4). IEEE.

[152] Süren, E., Heiding, F., Olegård, J., &Lagerström, R. (2023). PatrIoT: practical and agile threat research for IoT. International Journal of Information Security, 22(1), 213-233.

[153] Alsmadi, I. (2023). The NICE cyber security framework: Cyber security intelligence and analytics. Springer Nature.

[154] Bhol, S. G., Mohanty, J. R., &Pattnaik, P. K. (2023). Taxonomy of cyber security metrics to measure strength of cyber security. Materials Today: Proceedings, 80, 2274-2279.

[155] Liyanage, M., Braeken, A., Shahabuddin, S., &Ranaweera, P. (2023). Open RAN security: Challenges and opportunities. Journal of Network and Computer Applications, 214, 103621.

[156] Nyakomitta, S. P., &Omollo, V. (2014). Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE), 16(5), 137-44.

[157] Riegler, M., Sametinger, J., Vierhauser, M., &Wimmer, M. (2023). A model-based mode-switching framework based on security vulnerability scores. Journal of Systems and Software, 200, 111633.

[158] Sworna, Z. T., Babar, M. A., & Sreekumar, A. (2023, March). IRP2API: Automated Mapping of Cyber Security Incident Response Plan to Security Tools' APIs. In 2023 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER) (pp. 546-557). IEEE.

[159] Kraus, V. L. (2023). Adaptive Incident Response Plans for Cyber Resilience in Small and Medium Enterprises: Analysis and Increase of Cyber Security for a Small Enterprise by Designing an Incident Response Pl. In Handbook of Research on Cybersecurity Risk in Contemporary Business Systems (pp. 1-32). IGI Global.

[160] Woods, D. W., Böhme, R., Wolff, J., &Schwarcz, D. (2023). Lessons lost: incident response in the age of cyber insurance and breach attorneys. In Proceedings of the 32nd USENIX Security Symposium.

[161] Nyangaresi, V. O. (2021, September). Lightweight key agreement and authentication protocol for smart homes. In 2021 IEEE AFRICON (pp. 1-6). IEEE.

[162] De Lima, F. A., &Seuring, S. (2023). A Delphi study examining risk and uncertainty management in circular supply chains. International Journal of Production Economics, 258, 108810.

[163] Alhajjar, E., & Lee, K. (2022, June). The US Cyber Threat Landscape. In European Conference on Cyber Warfare and Security (Vol. 21, No. 1, pp. 18-24).

[164] Mathas, C. M., Grammatikakis, K. P., Vassilakis, C., Kolokotronis, N., Bilali, V. G., &Kavallieros, D. (2020, August). Threat landscape for smart grid systems. In Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-7).

[165] Tarun, R. (2022). Who Is Behind the Evolving Threat Landscape?.

[166] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11, 2(3): 399-406.

[167] Spencer Jr, B. F., Hoskere, V., &Narazaki, Y. (2019). Advances in computer vision-based civil infrastructure inspection and monitoring. Engineering, 5(2), 199-222.

[168] Aghili, S. F., Sedaghat, M., Singelée, D., & Gupta, M. (2022). MLS-ABAC: efficient multi-level security attribute-based access control scheme. Future Generation Computer Systems, 131, 75-90.

[169] Sriram, G. S., & Sriram, G. S. (2022). Security challenges of big data computing. International Research Journal of Modernization in Engineering Technology and Science, 4(1), 1164-1171.

[170] Creazza, A., Colicchia, C., Spiezia, S., &Dallari, F. (2022). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. Supply Chain Management: An International Journal, 27(1), 30-53.

[171] Nyangaresi, V. O., Ahmad, M., Alkhayyat, A., & Feng, W. (2022). Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems, 39(10), e13126.

[172] Liu, Z., Chen, X., & Yu, J. (2022). Adaptive sliding mode security control for stochastic Markov jump cyber-physical nonlinear systems subject to actuator failures and randomly occurring injection attacks. IEEE Transactions on Industrial Informatics, 19(3), 3155-3165.

[173] Sawik, T., &Sawik, B. (2022). A rough cut cybersecurity investment using portfolio of security controls with maximum cybersecurity value. International Journal of Production Research, 60(21), 6556-6572.

[174] Wichary, T., MongayBatalla, J., Mavromoustakis, C. X., Żurek, J., &Mastorakis, G. (2022). Network slicing security controls and assurance for verticals. Electronics, 11(2), 222.

[175] AlGhamdi, S., Win, K. T., &Vlahu-Gjorgievska, E. (2022). Employees' intentions toward complying with information security controls in Saudi Arabia's public organisations. Government Information Quarterly, 39(4), 101721.

[176] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Dec;11(4):66.

[177] Pishdar, M., DaneshShakib, M., Antucheviciene, J., &Vilkonis, A. (2021). Interval type-2 fuzzy super sbm network dea for assessing sustainability performance of third-party logistics service providers considering circular economy strategies in the era of industry 4.0. Sustainability, 13(11), 6497.

[178] Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., & Tatar, U. (2021). Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. Electronics, 10(10), 1168.

[179] Chen, Z. S., Zhang, X., Govindan, K., Wang, X. J., & Chin, K. S. (2021). Third-party reverse logistics provider selection: A computational semantic analysis-based multi-perspective multi-attribute decision-making approach. Expert Systems with Applications, 166, 114051.

[180] Li, F., Yu, X., Ge, R., Wang, Y., Cui, Y., & Zhou, H. (2021). BCSE: Blockchain-based trusted service evaluation model over big data. Big Data Mining and Analytics, 5(1), 1-14.

[181] Nyangaresi, V. O. (2022). Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture, 133, 102763.

[182] Irani, Z., Abril, R. M., Weerakkody, V., Omar, A., & Sivarajah, U. (2022). The impact of legacy systems on digital transformation in European public administration: Lesson learned from a multi case analysis. Government Information Quarterly, 101784.

[183] Tornhill, A. (2018). Software Design X-Rays: Fix Technical Debt with Behavioral Code Analysis. Software Design X-Rays, 1-200.

[184] Dekker, S., Hollnagel, E., Woods, D., & Cook, R. (2008). Resilience Engineering: New directions for measuring and maintaining safety in complex systems. Lund University School of Aviation, 1, 1-6.

[185] Gholami, M. F., Daneshgar, F., Beydoun, G., &Rabhi, F. (2017). Challenges in migrating legacy software systems to the cloud—an empirical study. Information Systems, 67, 100-113.

[186] Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., &Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. Electronics, 9(9), 1460.

[187] Nyangaresi, V. O. (2022, July). Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In 2022 International Conference on Inventive Computation Technologies (ICICT) (pp. 1-6). IEEE.

[188] Aldawood, H., & Skinner, G. (2018, December). Educating and raising awareness on cyber security social engineering: A literature review. In 2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE) (pp. 62-68). IEEE.

[189] Hart, S., Margheri, A., Paci, F., &Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. Computers & Security, 95, 101827.

[190] Caballero, A. (2017). Security education, training, and awareness. In Computer and information security handbook (pp. 497-505). Morgan Kaufmann.

[191] Furnell, S., &Vasileiou, I. (2017). Security education and awareness: just let them burn?. Network Security, 2017(12), 5-9.

[192] Aldawood, H., Alashoor, T., & Skinner, G. (2020). Does awareness of social engineering make employees more secure. International Journal of Computer Applications, 177(38), 45-49.

[193] Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. Education and Information Technologies, 26(2), 1721-1736.

[194] Nyangaresi, V. O. (2021, November). Provably secure protocol for 5G HetNets. In 2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) (pp. 17-22). IEEE.

[195] Dawson, J. K., Twum, F., HayfronAcquah, J. B., &Missah, Y. M. (2023). Ensuring confidentiality and privacy of cloud data using a non-deterministic cryptographic scheme. Plos one, 18(2), e0274628.

[196] Chen, C. M., Li, Z., Kumari, S., Srivastava, G., Lakshmanna, K., &Gadekallu, T. R. (2023). A provably secure key transfer protocol for the fog-enabled Social Internet of Vehicles based on a confidential computing environment. Vehicular Communications, 39, 100567.

[197] Khan, L. S., Khan, M., Hazzazi, M. M., & Jamal, S. S. (2023). A novel combination of information confidentiality and data hiding mechanism. Multimedia Tools and Applications, 82(5), 6917-6941.

[198] Ali, M., Jung, L. T., Sodhro, A. H., Laghari, A. A., Belhaouari, S. B., & Gillani, Z. (2023). A Confidentiality-based data Classification-as-a-Service (C2aaS) for cloud security. Alexandria Engineering Journal, 64, 749-760.

[199] Jin, C., Yang, Z., Xiang, T., Adepu, S., & Zhou, J. (2023). HMACCE: Establishing Authenticated and Confidential Channel from Historical Data for Industrial Internet of Things. IEEE Transactions on Information Forensics and Security.

[200] Nyangaresi, V. O., & Mohammad, Z. (2022, June). Session Key Agreement Protocol for Secure D2D Communication. In The Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 (pp. 81-99). Cham: Springer International Publishing.

[201] Suo, D., Mo, B., Zhao, J., & Sarma, S. E. (2023). Proof of Travel for Trust-Based Data Validation in V2I Communication. IEEE Internet of Things Journal.

[202] Veith, B., Krummacker, D., &Schotten, H. D. (2023). The road to trustworthy 6G: A survey on trust anchor technologies. IEEE Open Journal of the Communications Society, 4, 581-595.

[203] Petcu, A., Frunzete, M., &Stoichescu, D. A. (2023, March). A Practical Implementation Of A Digital Document Signature System Using Blockchain. In 2023 13th International Symposium on Advanced Topics in Electrical Engineering (ATEE) (pp. 1-6). IEEE.

[204] Singh, C. E. J., &Jagatheeswari, A. (2023). Secured blind digital certificate and LamportMerkle cloud assisted medical image sharing using blockchain. Multimedia Tools and Applications, 82(6), 9323-9342.

[205] Dewangan, N. K., Chandrakar, P., Kumari, S., & Rodrigues, J. J. (2023). Enhanced privacy-preserving in student certificate management in blockchain and interplanetary file system. Multimedia Tools and Applications, 82(8), 12595-12614.

[206] Yeshmuratova, A., &Amanbaev, N. (2023). Ensuring Computer Data and Management System Security. International Bulletin of Applied Science and Technology, 3(4), 282-287.

[207] Nyangaresi VO, Abduljabbar ZA, Al Sibahee MA, Ibrahim A, Yahya AN, Abduljaleel IQ, Abood EW. Optimized Hysteresis Region Authenticated Handover for 5G HetNets. InArtificial Intelligence and Sustainable Computing: Proceedings of ICSISCET 2021 2022 Nov 16 (pp. 91-111). Singapore: Springer Nature Singapore.

[208] Abbasi, M., Plaza-Hernández, M., &Mezquita, Y. (2023, January). Security of IoT Application Layer: Requirements, Threats, and Solutions. In Ambient Intelligence—Software and Applications—13th International Symposium on Ambient Intelligence (pp. 86-100). Cham: Springer International Publishing.

[209] Fischer, M., &Tönjes, R. (2023). Modelling of Resource-Aware Information Flows for Resource Constraint IoT Devices. In Internet of Things: 5th The Global IoT Summit, GIoTS 2022, Dublin, Ireland, June 20–23, 2022, Revised Selected Papers (pp. 302-314). Cham: Springer International Publishing.

[210] Amro, A., &Gkioulos, V. (2023). Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. International Journal of Information Security, 22(1), 249-288.

[211] Khanna, K., Ravikumar, G., &Govindarasu, M. (2023, February). Defense-in-depth framework for power transmission system against cyber-induced substation outages. In 2023 IEEE Texas Power and Energy Conference (TPEC) (pp. 1-6). IEEE.

[212] Batool, M., Alotaibi, S. S., Alatiyyah, M. H., Alnowaiser, K., Aljuaid, H., Jalal, A., & Park, J. (2023). Depth sensors-based action recognition using a modified K-ary entropy classifier. IEEE Access.

[213] Huang, Y., Li, Y. J., & Cai, Z. (2023). Security and privacy in metaverse: A comprehensive survey. Big Data Mining and Analytics, 6(2), 234-247.

[214] Nyangaresi, V. O. (2021, September). ECC based authentication scheme for smart homes. In 2021 International Symposium ELMAR (pp. 5-10). IEEE.

[215] Rajadevi, R., Venkatachalam, K., Masud, M., AlZain, M. A., &Abouhawwash, M. (2023). Proof of Activity Protocol for IoMT Data Security. Computer Systems Science & Engineering, 44(1).

[216] Pattnaik, N., Li, S., & Nurse, J. R. (2023). A Survey of User Perspectives on Security and Privacy in a Home Networking Environment. ACM Computing Surveys, 55(9), 1-38.

[217] Zhu, Y., Li, G., Guo, Y., Li, D., &Bohlooli, N. (2023). Modeling Optimal Energy Exchange Operation of Microgrids Considering Renewable Energy Resources, Risk-based Strategies, and Reliability Aspect Using Multi-objective Adolescent Identity Search Algorithm. Sustainable Cities and Society, 91, 104380.

[218] Pramod, D. (2023). Privacy-preserving techniques in recommender systems: state-of-the-art review and future research agenda. Data Technologies and Applications, 57(1), 32-55.

[219] Aljabhan, B., &Obaidat, M. A. (2023). Privacy-Preserving Blockchain Framework for Supply Chain Management: Perceptive Craving Game Search Optimization (PCGSO). Sustainability, 15(8), 6905.

[220] Zhong, H., Gu, C., Zhang, Q., Cui, J., Gu, C., & He, D. (2023). Conditional privacy-preserving message authentication scheme for cross-domain Industrial Internet of Things. Ad Hoc Networks, 144, 103137.

[221] Nyangaresi, V. O., Abd-Elnaby, M., Eid, M. M., &NabihZakiRashed, A. (2022). Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies, 33(9), e4528.

[222] Almomani, I., El-Shafai, W., AlKhayer, A., Alsumayt, A., Aljameel, S., & Alissa, K. (2023). Proposed biometric security system based on deep learning and chaos algorithms. Comput. Mater. Contin., 74(2), 3515-3537.

[223] Elazm, L. A. A., El-Shafai, W., Ibrahim, S., Egila, M. G., Shawkey, H., Elsaid, M. K., ... & El-Samie, F. E. A. (2023). Efficient Hardware Design of a Secure Cancellable Biometric Cryptosystem. Intelligent Automation & Soft Computing, 36(1).

[224] Abdulrahman, S. A., &Alhayani, B. (2023). A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. Materials Today: Proceedings, 80, 2642-2646.

[225] Joo, M., Kim, S. H., Ghose, A., & Wilbur, K. C. (2023). Designing Distributed Ledger technologies, like Blockchain, for advertising markets. International Journal of Research in Marketing, 40(1), 12-21.

[226] Laghari, A. A., Khan, A. A., Alkanhel, R., Elmannai, H., &Bourouis, S. (2023). Lightweight-biov: blockchain distributed ledger technology (bdlt) for internet of vehicles (iovs). Electronics, 12(3), 677.

[227] Al Sibahee, M. A., Ma, J., Nyangaresi, V. O., &Abduljabbar, Z. A. (2022, June). Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-6). IEEE.

[228] Sangaiah, A. K., Javadpour, A., Ja'fari, F., Pinto, P., Zhang, W., & Balasubramanian, S. (2023). A hybrid heuristics artificial intelligence feature selection for intrusion detection classifiers in cloud of things. Cluster Computing, 26(1), 599-612.

[229] Dostonbek, T., & Jamshid, M. (2023). Use of Artificial Intelligence Opportunities for Early Detection of Threats to Information Systems. Central Asian Journal of Theoretical and Applied Science, 4(4), 93-98.

[230] Jain, J. K., &Waoo, A. A. (2023). An Artificial Neural Network Technique for Prediction of Cyber-Attack using Intrusion Detection System. Journal of Artificial Intelligence, Machine Learning and Neural Network (JAIMLNN) ISSN: 2799-1172, 3(02), 33-42. Samtani, S., Zhao, Z., & Krishnan, R. (2023). Secure Knowledge Management and Cybersecurity in the Era of Artificial Intelligence. Information Systems Frontiers, 25(2), 425-429.

[231] Selvarajan, S., Srivastava, G., Khadidos, A. O., Khadidos, A. O., Baza, M., Alshehri, A., & Lin, J. C. W. (2023). An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. Journal of Cloud Computing, 12(1), 38.

[232] Nyangaresi, V. O., El-Omari, N. K. T., &Nyakina, J. N. (2022). Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research, 4(1), 10-19.

[233] Borgogno, O., & Colangelo, G. (2019). Data sharing and interoperability: Fostering innovation and competition through APIs. Computer Law & Security Review, 35(5), 105314.

[234] Jin, H., Xu, C., Luo, Y., Li, P., Cao, Y., & Mathew, J. (2019, December). Toward secure, privacy-preserving, and interoperable medical data sharing via blockchain. In 2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS) (pp. 852-861). IEEE.

[235] Hao, K., Xin, J., Wang, Z., Yao, Z., & Wang, G. (2023). Efficient and Secure Data Sharing Scheme on Interoperable Blockchain Database. IEEE Transactions on Big Data.

[236] Khan, A. A., &Abonyi, J. (2022). Information sharing in supply chains-Interoperability in an era of circular economy. Cleaner Logistics and Supply Chain, 100074.

[237] ZakiRashed A.N., Ahammad S.H., Daher M.G., Sorathiya V., Siddique A., Asaduzzaman S., Rehana H., Dutta N., Patel S.K., Nyangaresi V.O., Jibon R.H. (2022). Signal propagation parameters estimation through designed multi layerfibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications, (0).

[238] Mohy-eddine, M., Guezzaz, A., Benkirane, S., &Azrour, M. (2023). An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection. Multimedia Tools and Applications, 1-19.

[239] Yazdinejad, A., Dehghantanha, A., Parizi, R. M., Srivastava, G., &Karimipour, H. (2023). Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks. Computers in Industry, 144, 103801.

[240] Aldhyani, T. H., &Alkahtani, H. (2023). Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. Mathematics, 11(1), 233.

[241] Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. Computers & Security, 87, 101589.

[242] Honi, D. G., Ali, A. H., Abduljabbar, Z. A., Ma, J., Nyangaresi, V. O., Mutlaq, K. A. A., & Umran, S. M. (2022, December). Towards Fast Edge Detection Approach for Industrial Products. In 2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) (pp. 239-244). IEEE.

[243] Rostami, E., Karlsson, F., & Gao, S. (2023). Policy components–a conceptual model for modularizing and tailoring of information security policies. Information & Computer Security.

[244] Kitsios, F., Chatzidimitriou, E., &Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. Sustainability, 15(7), 5828.

[245] Sivan-Sevilla, I. (2023). Supranational security states for national security problems: governing by rules & capacities in tech-driven security spaces. Journal of European Public Policy, 30(7), 1353-1378.

[246] Mayer, B. (2019). A review of the literature on community resilience and disaster recovery. Current environmental health reports, 6, 167-173.

[247] Huq, M. E., Sarker, M. N. I., Prasad, R., Kormoker, T., Hossain, M. A., Rahman, M. M., & Al Dughairi, A. A. (2021). Resilience for disaster management: opportunities and challenges. Climate vulnerability and resilience in the global south: human adaptations for sustainable futures, 425-442.